Trading Privacy for Angry Birds: A Call for Courts to Reevaluate Privacy Expectations in Modern Smartphones

Jeremy Andrew Ciarabellini[*]

"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."[1]

"New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[2]

"There is nothing concealed that will not be disclosed, or hidden that will not be made known. What you have said in the dark will be heard in the daylight, and what you have whispered in the ear in the inner rooms will be proclaimed from the roofs."[3]

I. INTRODUCTION

Of all the smartphone uses, the calling function is probably used the least. Rather, individuals more commonly use their smartphone for surfing the web, checking Facebook, and playing games. Highlighting the "smart" in smartphone, these phones often know more about their users'

[*] J.D. Candidate, May 2015, Seattle University School of Law; B.A., United States Politics and Government, University of Puget Sound. I would like to thank my wife for all of her love and support as this Note stole me away from home for many hours.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

2. United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring).

3. *Luke* 12:2–3 (New International Version).

daily activities than the users. Without requiring any sort of input, smartphones can tell the user how many steps they walk each day, when it is time to leave for work (also, of course, determining the traveling time with the most up-to-date traffic reports), and when an item recently ordered on Amazon will be delivered. Smartphone users may instinctively know that they could dig into their phones' settings and turn off these features. They may also know that if their phones are telling them information about their daily activities, they are likely sharing that same information with third parties—targeted advertisements come to mind. Of course, all of the downloaded "apps" had some sort of agreement that the user probably did not read and just clicked "yes." The reality is that people enjoy the conveniences offered by smartphones and give little thought to any privacy implications. In practice, it seems smartphone users are willing to trade their privacy to play Angry Birds.

First introduced to the public in 1983,[4] cell phones have evolved to now allow average citizens to carry internet-connected computers in their pockets.[5] With such rapid technology advancement, it is unsurprising that the legal system has yet to establish a consistent privacy-based jurisprudence when it comes to smartphones and government searches.[6] Currently, courts are examining governmental searches of private smartphones under the Fourth Amendment.[7] However, the problem is that when the courts analyze the legality of a warrantless smartphone search by police, they summarily assume that the predicate "reasonable expectation of privacy" requirement exists for there to be a "search" within the meaning of the Fourth Amendment. Courts then move directly into analyzing whether the search was appropriate under an exception to the warrant requirement—this most commonly being the "search incident to arrest" excep-

4. *Cell Phone Timeline*, SOFTSCHOOLS, http://www.softschools.com/timelines/cell_phone_timeline/28/ (last visited Mar. 24, 2014). Motorola released the first cell phones ten years after Dr. Martin Cooper invented the first handheld phone that did not need to be powered through a car. *See id.*

5. The growth of cell phone technology was very rapid. In 1989, Motorola introduced the first flip phone, and by 1993 text messaging was invented. *Id*. In 2002, Sanyo produced the first camera phones, which allowed users to connect their phones to a computer and print their pictures. *Id*. And in a move that will likely be seen as changing the course of human history, Apple released the first iPhone in 2007. *Id*. The iPhone allowed users to perform on their cell phone almost any task that could be performed on their home computers. *Id.*

6. *See infra* Parts III, IV. "Greater discussion of this topic is due to both increased cell phone usage and constantly evolving cell phone technology." Ashley B. Snyder, Comment, *The Fourth Amendment and Warrantless Cell Phone Searches: When Is Your Cell Phone Protected?*, 46 WAKE FOREST L. REV. 155, 162 (2011).

7. *See infra* Parts III–V.

tion.[8] Similarly, scholars are also guilty of making this assumption about privacy expectations.[9]

It is the position of this Note that courts need to take a step back in their Fourth Amendment analysis and carefully evaluate whether individuals do in fact have the requisite privacy expectations. Specifically, this Note argues that with the advancement in smartphone technology and the ubiquity of privacy waivers in "apps," smartphone users too often share their personal information to third parties to reasonably claim any general expectation of privacy to the data in their smartphones. Individuals have traded the convenience of smartphones at the expense of their privacy.

In this Note, Part II examines the privacy protections of the Fourth Amendment and the history of the search incident to arrest exception to the warrant requirement. Part III surveys how various lower courts explore privacy rights in smartphones/cell phones and apply the search incident to arrest exception.[10] Part IV describes two fairly recent Supreme Court decisions that call for an examination of privacy expectations in smartphones and how the scholarly commentary on those decisions mistakenly maintains the primary focus on the search incident to arrest exception. Part V looks at the Supreme Court's most recent smartphone/cell phone search case and its failure to examine privacy expectations. Part VI presents data that modern smartphones users continue to download apps despite the ubiquity of privacy waivers. Part VII argues that an application of the third-party doctrine may vitiate any argument that an expectation of privacy in modern smartphones exists. Part VIII concludes.

II. THE FOURTH AMENDMENT AND THE SEARCH INCIDENT TO ARREST EXCEPTION

The Fourth Amendment states that it is "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[11] The framers' policy reasoning behind this Amendment was the desire to have magistrates, rather than law enforcement, determine the permissibility and limitations of searches and

8. *See infra* Part III.

9. *See infra* Part IV.B.

10. While there is no standard definition of "smartphone" within the mobile phone industry, this Note uses the term in reference to mobile phones containing an operating system and capable of downloading apps. *See* Adam Fendelman, *How Are Cell Phones Different From Smartphones?*, ABOUT TECH, http://cellphones.about.com/od/coveringthebasics/qt/cellphonesvssmartphones.htm (last visited Mar. 17, 2015).

11. U.S. CONST. amend. IV.

seizures.[12] This policy comes from the belief that magistrates, not law enforcement, are best able "[t]o provide the necessary security against unreasonable intrusions upon the private lives of individuals."[13] As such, "where there is a [reasonable] expectation of privacy, and no warrant is obtained, the search or seizure is generally illegal, and the evidence obtained thereby is generally excluded, unless an exception to the warrant requirement applies."[14] However, a warrant is not required where there is no search within the meaning of the Fourth Amendment—i.e., where there is no reasonable expectation of privacy in the object being searched.[15]

Therefore, as the threshold inquiry for determining whether an individual has a reasonable expectation of privacy in the object being searched, the court asks the following two questions: (1) does the individual subjected to the search exhibit an actual expectation of privacy, and (2) is that expectation one "that society is prepared to recognize as reasonable."[16] This test originates from Justice Harlan's concurrence in *Katz v. United States* and is commonly referred to as the *Katz* test.[17] This test "is not capable of precise definition or mechanical application."[18] In essence, the Fourth Amendment reasonableness analysis requires balancing the State's need to conduct searches and the individual's right to privacy.[19] Should the court recognize a privacy expectation, it then analyzes whether an exception to the warrant requirement exists.

Although the Supreme Court has held that warrantless searches (where a recognized privacy interest exists) are per se unreasonable,[20] the Court recognizes many exceptions.[21] One of these exceptions is the search incident to arrest.[22] The search incident to arrest exception to the warrant requirement permits government agents to search a person and his belongings upon a valid arrest to ensure officer safety and to preserve

12. McDonald v. United States, 335 U.S. 451, 455–56 (1948).

13. Chimel v. California, 395 U.S. 752, 758–59 (1969) (quoting Trupiano v. United States, 334 U.S. 699, 705, 708 (1948)).

14. 22A C.J.S. *Criminal Law* § 1066 (2015).

15. *See* Illinois v. Rodriguez, 497 U.S. 177, 183–84 (1990) (regarding the exceptions); Illinois v. Andreas, 463 U.S. 765, 771 (1983) (regarding the expectation of privacy); *see also* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

16. Oliver v. United States, 466 U.S. 170, 177 (1984) (quoting Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

17. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

18. Bell v. Wolfish, 441 U.S. 520, 559 (1979).

19. *See id.*

20. California v. Acevedo, 500 U.S. 565, 592–93 (1982).

21. 3A CHARLES ALAN WRIGHT, ANDREW D. LEIPOLD, PETER J. HENNING & SARAH N WELLING, FEDERAL PRACTICE & PROCEDURE CRIMINAL § 675 (4th ed. 2010).

22. *Id.*

evidence.[23] This exception is the most commonly litigated issue of warrantless smartphone/cell phone searches.

Courts applying the search incident to arrest exception to warrantless smartphone/cell phone searches do not apply the exception uniformly.[24] While this section details the history of the search incident to arrest exception and how it came to be applied to cell phone searches, it is remarkable that courts largely overlook the threshold question—whether there is a reasonable expectation of cell phone privacy[25]—and jump almost directly into search incident to arrest analysis.

The Supreme Court's early jurisprudence on the search incident to arrest exception is unclear and primarily mentioned in dicta.[26] However, the Court explicitly established this exception in *Chimel v. California* in 1969.[27] In *Chimel*, officers arrived at the house of the defendant to serve an arrest warrant for a coin shop burglary.[28] When the officers handed the defendant the warrant, they asked for permission to "look around" the house.[29] Although the defendant objected, the officers conducted a search of the home, even though they had no warrant to do so.[30] For nearly an hour, the officers searched the entire house, directing the defendant's wife to open various drawers and move the contents around so they could thoroughly see what was inside.[31] The officers seized numerous items, including the stolen coins.[32] Over the defendant's objections that the items were unconstitutionally seized and admitted into evidence, the defendant was convicted of the burglary.[33] On appeal, the Supreme Court announced that

---

23. Sara M. Corradi, Comment, *Be Reasonable! Limit Warrantless Smart Phone Searches to* Gant*'s Justification for Searches Incident to Arrest*, 63 CASE W. RES. L. REV. 943, 945 (2013).

24. *See infra* Parts III, IV.B.

25. Put another way, whether the Fourth Amendment applies in the first place.

26. *See* Chimel v. California, 395 U.S. 752, 770 (1969) (White, J., dissenting) (citing Weeks v. United States, 232 U.S. 383, 392 (1914) (stating that there is a right of the government "under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidence of crime.")); Carroll v. United States, 267 U.S. 132, 755–56 (1969) ("When a man is legally arrested for an offense, whatever is found upon his person or in his control which it is unlawful for him to have and which may be used to prove the offense may be seized and held as evidence in the prosecution."). *See also* Marron v. United States, 275 U.S. 192, 199 (1927); Angello v. United States, 269 U.S. 20, 30 (1925).

27. *Chimel*, 395 U.S. at 763.

28. *Id.* at 753.

29. *Id.*

30. *Id.* at 753–54.

31. *Id*. at 754.

32. *Id.*

33. *Id.*

> [w]hen an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the [arrestee] might seek to use in order to resist arrest or effect his escape. . . . And the area into which an arrestee might reach in order to grab a weapon or evidentiary items must, of course, be governed by a like rule. . . . There is ample justification, therefore, for a search of the arrestee's person and the area "within his immediate control" . . . .[34]

However, applying the rule to the case, the Court held that the search of the defendant's house went "far beyond" the defendant's person and his immediate area; therefore, the search was not reasonable.[35]

Four years after *Chimel*, the Court expanded the search incident to arrest exception in *United States v. Robinson*.[36] In *Robinson*, the defendant was pulled over and subsequently arrested for driving with a revoked license.[37] The officer searched the defendant's person and found a cigarette package in the defendant's coat pocket.[38] Being able to feel that the package contained something other than cigarettes, the officer opened the package and found heroin.[39] The heroin was admitted into evidence and used to convict the defendant of a drug offense.[40] On appeal, the Supreme Court held that the officer was "entitled" to inspect the cigarette package because the search was incident to a valid arrest; therefore, the discovered heroin was properly seized and admitted into evidence.[41] The Court concluded that the search was reasonable, even without a concern about the loss of evidence or officer safety, because "[h]aving in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it."[42] The Court's holding in *Robinson* establishes that the search incident to arrest exception is "limited to personal property . . . immediately associated with the person of the arrestee."[43]

Although the Supreme Court did not specifically address this exception in the context of smartphones/cell phones until 2014 in *Riley v.*

---

34. *Id.* at 762–63.
35. *Id.* at 768.
36. United States v. Robinson, 414 U.S. 218 (1973).
37. *Id.* at 220.
38. *Id.* at 222–23.
39. *Id.* at 223.
40. *Id.*
41. *Id.* at 236.
42. *Id.*
43. Riley v. California, 134 S. Ct. 2473, 2484 (2014) (quoting United States v. Chadwick, 433 U.S. 1, 15 (1977)) (internal quotation marks omitted).

California,[44] there was precedent set in the interim involving other emerging technologies such as wiretapping,[45] aerial photography,[46] thermal detection,[47] and GPS monitoring.[48] The Court's examination of a warrantless search of a pager in *City of Ontario, Cal. v. Quon* is perhaps most analogous to a cell phone search.[49]

In *Quon*, the City of Ontario, California employed the petitioner as a police officer.[50] In 2001, the City issued the petitioner a pager to send and receive work-related text messages.[51] However, before giving the pager to the petitioner, the City announced a "computer policy" that specified that the City "reserve[d] the right to monitor and log all network activity including e-mail and internet use, with or without notice," and the employees should not expect any privacy when using such items.[52] While the policy did not apply to text messages on its face, the City did tell its employees—including the petitioner—that it would treat text messages as falling under the computer policy.[53] Soon after receiving the pager, the petitioner went over his monthly text message limit.[54] Initially, the City told the petitioner that it did not intend on auditing his text messages to see if the overage was due to personal use, suggesting that the petitioner could pay for the overage costs rather than have to go through an audit process.[55] As such, the petitioner continued to exceed the limits over the following months and reimbursed the City each time.[56] However, the City ultimately decided to audit the petitioner's text messages to evaluate whether the overages were due to personal use or whether the existing text message limit was too low.[57] The City discovered that the many of the petitioner's messages were personal—some sexually explicit—and determined that the petitioner was violating the City's policy.[58] The City disciplined the petitioner for the violations.[59]

---

44. *See id.* at 2480.
45. *See* Mitchell v. Forsyth, 472 U.S. 511, 530–31 (1985).
46. *See* Dow Chem. Co. v. United States, 476 U.S. 227, 234–39 (1986).
47. *See* Kyllo v. United States, 533 U.S. 27, 46 (2001).
48. *See* United States v. Jones, 132 S. Ct. 945, 952–54 (2012).
49. City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010).
50. *Id.* at 750.
51. *Id.* at 751.
52. *Id.*
53. *Id.*
54. *Id.* at 752.
55. *Id.*
56. *Id.*
57. *Id.*
58. *Id.* at 752–53.
59. *Id.* at 753.

The petitioner filed a suit against the City in federal court alleging that the City violated his Fourth Amendment right by obtaining and reviewing his text messages without a warrant.[60] Before the Supreme Court considered the specific issue presented, it noted that the Court "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[61] The Court further noted that "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior."[62] In its comments, the Court cannot have anticipated the truthfulness of the following words, written just one year into the iPhone era:

> Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own.[63]

Before reaching the merits of the case, the Court assumed, arguendo, that the petitioner did have a reasonable expectation of privacy in the text messages, and that the search performed fell within the meaning of the Fourth Amendment.[64] Ultimately, the Court held that the search was reasonable under the "special needs" of the workplace exception for warrantless searches.[65] However, the Court's assumption that there was a privacy expectation left the opinion's discussion of cell phone and text message privacy as merely dicta. Without a firm standard set by the Supreme Court, lower courts were left to develop their own warrantless cell phone, and eventually smartphone, search jurisprudence. Unfortunately, many lower courts have followed the Supreme Court's example and just assumed that a privacy right exists in smartphones/cell phones.

---

60. *Id.* at 754.

61. *Id.* at 759 (citing Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967)).

62. *Id.*

63. *Id.* at 760.

64. *Id.*

65. *Id.* at 761–62.

III. THE LOWER COURTS RECOGNIZE A PRIVACY INTEREST AND APPLY THE EXCEPTION

Before the Supreme Court decided that the search incident to arrest exception does not apply to smartphones/cell phones (skipping the preliminary question of whether a Fourth Amendment "search" occurred at all),[66] the lower courts came to varying conclusions. Remarkably, the fast-developing technology forced courts of all levels to hear smartphone/cell phone cases even before the Supreme Court in *Quon* was able to comment on privacy implications.[67] The leading lower court decision in this area is *United States v. Finley*.[68] Contextually, *Finley* is important because it was issued the same year that Apple released the first iPhone.[69] While the Fifth Circuit applied the correct test in determining both whether there was a privacy interest in the cell phone and whether there was a proper search of the cell phone incident to arrest, the court was in no position to anticipate how the iPhone and "app" agreements would change everything. Furthermore, the *Finley* decision also unfortunately led other courts to adopt the assumption that there is a privacy right in modern cell phones without employing appropriate analysis in the context of the post-iPhone era.

In *Finley*, the defendant was convicted of possession of methamphetamine with intent to distribute.[70] The conviction was the result of the defendant's arrest after he drove another defendant to a controlled purchase conducted by local and federal law enforcement.[71] After the arrest, officers seized and searched a cell phone that was located in the defendant's pocket.[72] Although the cell phone belonged to the defendant's employer, the defendant was also permitted to use the cell phone for personal use.[73] At trial, a federal law enforcement officer testified that several of the text messages found in the phone related to drug use and trafficking.[74] On appeal, the defendant asserted that the recovered text messages from the warrantless search of his phone should have been sup-

66. *See* discussion *infra* Part V.

67. United States v. Finley, 477 F.3d 250 (5th Cir. 2007). *Quon* was arguably the Supreme Court's leading cell phone privacy case until, perhaps, *Gant* and *Jones*. However, *Quon* was decided in 2010, a relatively late era in cell phone technology as the iPhone was already three years old at that point. The leading lower court decision, *Finley*, came in 2007—the same year that the iPhone was released.

68. *Id.*

69. *See supra* note 5 and accompanying text.

70. *Finley*, 477 F.3d at 255.

71. *Id.* at 253–54.

72. *Id.* at 254.

73. *Id.*

74. *Id.*

pressed at the trial.[75] Although the Fifth Circuit ultimately allowed the text messages into evidence, it did hold that there was a privacy interest in the cell phone.

In its analysis, the Fifth Circuit first had to decide whether the defendant had standing to challenge the search of his cell phone by having a reasonable expectation of privacy in the cell phone.[76] To test for the reasonable expectation of privacy, the court asked "(1) whether the defendant is able to establish an actual, subjective expectation of privacy with respect to the place being searched or items being seized, and (2) whether that expectation of privacy is one which society would recognize as reasonable."[77] Under this test, the court looks, in part, to whether there is a property or possessory interest in the thing being searched, whether there is a subjective privacy expectation that there would be no governmental intrusion, and whether there were measures taken to maintain privacy.[78] The court found that the defendant did have a reasonable expectation of privacy in the cell phone because, even though the defendant expected his employer to read his text messages, he maintained possession of the cell phone and could have reasonably expected to be free from intrusion by both the government and the general public.[79]

Next, the court held that the search of the cell phone was a lawful search incident to arrest.[80] The court reasoned, "It is well settled that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a reasonable search under that Amendment."[81] The court continued, "Police officers are not constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial."[82] Noting that the scope of

75. *Id.* at 258.

76. *Id.*

77. *Id.* (quoting United States v. Cardoza-Hinojosa, 140 F.3d 610, 614 (5th Cir. 1998)). Note that this is Justice Harlan's *Katz* test. *See supra* text accompanying note 17.

78. *Id.* at 258–59 (citing United States v. Ibarra, 948 F.2d 903, 906 (5th Cir. 1991)).

79. *Id.* at 259.

80. *Id.* at 259–60.

81. *Id.* at 259 (internal quotation marks and citations omitted).

82. *Id.* at 259–60 (internal quotation marks and citations omitted).

the search extends to containers found on the arrestee's person,[83] the court held that the search was proper.[84]

The court rejected the defendant's argument that the officers needed a warrant to search the phone because it was tantamount to a closed container by reaffirming that containers, even closed containers, may be searched pursuant to a valid custodial arrest.[85] Also important to the court's holding was its finding that a cell phone "does not fit into the category of 'property not immediately associated with [the defendant's] person' because it was on his person at the time of his arrest."[86] As a gloss to the search incident to arrest rule, this distinction is important because "[o]nce law enforcement officers have reduced . . . personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident to arrest"; therefore, the search of the property would then require a warrant.[87] By holding that a cell phone is immediately associated with the defendant's person, the court found that the search of the cell phone incident to arrest was proper.[88]

However, not all courts have followed *Finley*'s reasoning. For example, in the Northern District of California case of *United States v. Park*, San Francisco police narcotics officers had a warrant to search a home.[89] After executing the warrant, the officers arrested the defendants and transported them to the police station for booking.[90] After the defendants were booked and their cell phones were placed into evidence, the police searched the contents of their cell phones at the police sta-

---

83. *Id.* at 260 (citing United States v. Johnson, 846 F.2d 279, 282 (5th Cir. 1988) (per curiam); New York v. Belton, 453 U.S. 454, 460–61 (1981) (holding that containers within the arrestee's reach may be searched); United States v. Robinson, 414 U.S. 218, 223–24 (1973) (upholding the search of a cigarette package found on the arrestee's person)).

84. *Id.*

85. *Id.*

86. *Id.* at 260 n.7 (quoting United States v. Chadwick, 433 U.S. 1, 15 (1977)).

87. *See Chadwick*, 433 U.S. at 15.

88. *Finley*, 477 F.3d at 260. Many courts have adopted the *Finley* approach. Shortly after the *Finley* decision, the Fourth and Seventh Circuits adopted its reasoning, and upheld as constitutional the search of cell phones incident to arrest on the theory of preserving evidence. *See* United States v. Young, 278 F. App'x 242 (4th Cir. 2008) (per curiam). *See also* United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012) (upholding the search of a cell phone as a valid search incident to arrest where the sole purpose of the search was to find the phone's number); United States v. Murphy, 552 F.3d 405 (4th Cir. 2009) (holding that storage capacity does not affect whether a search is constitutional).

89. United States v. Park, No. CR 05-375SI, 2007 WL 1521573 *1 (N.D. Cal. May 23, 2007).

90. *Id.* at *2.

tion.[91] Rejecting the reasoning in *Finley*, the court held that the search was not proper as a search incident to arrest because "cellular phones should be considered 'possessions within an arrestee's immediate control' and not part of 'the person.'"[92] While the court noted that *Finley* was distinguishable because there the search was conducted at the location of the arrest, and here the search was conducted after booking, thus not meeting the "contemporaneous" requirement of *Chadwick*, the *Park* court relied more on the large storage capabilities of modern cell phones[93] and a policy argument that they should never be considered part of "the person," only "possessions within an arrestee's immediate control."[94] The court argued that a contrary holding would have "far-ranging consequences" because modern cell phones—which the court argued were more in line with personal computers—contain vast amounts of personal information and a search of such phones would go beyond the original "evidence protection" rationale for searches incident to arrest.[95]

Tellingly, the *Park* court never overtly considered whether the defendant had a reasonable expectation of privacy in the cell phone in the first place. The court seemed to have assumed that there was such an expectation because of the amount of information contained in the cell phone, and it proceeded directly to determining whether an exception to the search warrant requirement applied.[96] The court did not consider whether the defendants exhibited a subjective expectation of privacy in the cell phone or whether that expectation was one that society was prepared to accept as reasonable. The court did not even mention how the defendants used and treated the data stored in their cell phones. In fact, the mistake of assuming that there is a reasonable expectation of privacy in cell phones, and now smartphones, without giving the issue its due analysis, is a common one.

---

91. *Id.* at *3.

92. *Id.* at *8 (citing *Chadwick*, 433 U.S. at 16 n.10).

93. *Id.* ("This is so because modern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages."). *Id.* Note that this case refers to cell phones, but its reasoning and description of cell phone capabilities could easily be attributed to smartphones.

94. *Id.*

95. *Id.*

96. *Id.* Presumably, even if the court did analyze whether there was a privacy interest in the cell phone, the analysis would be outdated. Like *Finley*, this opinion was issued in 2007, the same year the iPhone was released. Thus, *Park* would have similarly not been able to anticipate the changes the iPhone heralded. *See supra* note 5 and accompanying text.

For example, in *State v. Smith*, the Ohio Supreme Court had to determine whether the search of a cell phone found on the person of an arrestee accused of being a drug dealer was constitutional as a search incident to arrest.[97] After first acknowledging that *Finley* and *Park* provide the leading framework for this issue, the court recognized that "[g]iven the continuing rapid advancements in cell phone technology . . . there are legitimate concerns regarding the effect of allowing warrantless searches of cell phones, especially so-called smart phones, which allow for high-speed Internet access and are capable of storing tremendous amounts of private data."[98] Initially, the court rejected a distinction between the defendant's "standard" phone and "smart phones."[99] The defendant in this case did not have what is considered a conventional "smart phone."[100] However, the court noted that modern "standard" cell phones, not just smartphones, are capable of performing much more complex tasks than traditional phones, for example, sending text messages, storing information, and taking pictures.[101] On this reasoning, the court declined to distinguish between modern "traditional" cell phones and "smart phones."[102] From there, the court determined that a cell phone's ability to store large amounts of data is what gives the phone's owner "a reasonable and justifiable expectation of a higher level of privacy in the information they contain."[103] Like the *Finley* court, the court here failed to consider how the defendant *used and treated* the information in his cell phone as a consideration for determining whether a reasonable expectation of privacy existed.

---

97. State v. Smith, 920 N.E. 2d 949, 950–51 (Ohio 2009).

98. *Id.* at 954.

99. *Id.*

100. *Id.* at 956.

101. *Id.* at 954.

102. *Id.* The court determined not to draw a legal distinction between smartphones and modern "standard" cell phones because of their overlapping capabilities. *Id.* ("[W]e note that in today's advanced technological age many 'standard' cell phones include a variety of features above and beyond the ability to place phone calls. Indeed, . . . many cell phones give users the ability to send text messages and take pictures. Other modern 'standard' cell phones can also store and transfer data and allow users to connect to the Internet. Because basic cell phones in today's world have a wide variety of possible functions, it would not be helpful to create a rule that requires officers to discern the capabilities of a cell phone before acting accordingly."). *Id.*

103. *Id.* at 955. Other courts have also relied on the storage capacity of cell phones for finding a reasonable expectation of privacy. *See, e.g.*, United States v. Zavala, 514 F.3d 562, 577 (5th Cir. 2008); Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012) (holding that an expectation of privacy exists because modern cell phones hold large amounts of private information, including "phonebook information, appointment calendars, text messages, call logs, photographs, audio and video recordings, web browsing history, electronic documents and user location information."). *But see* People v. Diaz, 244 P.3d 501, 508–09 (Cal. 2011) (rejecting the storage capacity reasoning as too subjective to particular items).

As illustrated above, the real problem lies in how the courts are determining that there is a reasonable expectation of privacy in smartphones/cell phones. Courts are either not giving the issue sufficient analysis—*Smith*, for example—or are merely assuming that a privacy interest exists—*Park*, for example.[104] Even where courts do test whether the Fourth Amendment applies, the tests are based on outmoded cell phone paradigms.[105] Indeed, a thorough and honest inquiry into the Fourth Amendment's applicability to smartphone searches may not occur if courts refuse to analyze the possible legal significance of the difference between smartphones and cell phones.[106] However, after the lower courts split on their analyses,[107] some scholars believed that a pair of United States Supreme Court decisions offered guidance towards a uniform national method of analyzing the warrantless search of smartphones/cell phones.[108]

IV. *GANT*, *JONES*, AND THE FUTURE OF CELL PHONE SEARCHES?

A. The Gant *and* Jones *Decisions*

Some commenters believe that the Supreme Court's holdings in *Arizona v. Gant*[109] and *United States v. Jones*[110] foreshadowed the Court's future warrantless smartphone/cell phone search jurisprudence.[111] However, even these cases assume that the Fourth Amendment protects these searches and they continue to focus on the search incident to arrest exception.

The *Gant* decision greatly limited the areas in which police may search under the search incident to arrest doctrine. Later, courts used *Gant* as a basis for limiting searches of cellphones.[112] In *Gant*, after the defendant was arrested for driving with a suspended license, police offic-

104. *See Smith*, 920 N.E. 2d at 950–51. *See also* Eunice Park, *Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search-Incident-To-Arrest Exception to the Cell Phone as "Hybrid"*, 60 DRAKE L. REV. 429, 460 (2012) ("Most courts that have held a warrantless cell phone search was reasonable did not extensively discuss the expectation of privacy."). *See, e.g.*, United States v. Park, No. CR 05-375SI, 2007 WL 1521573 *1 (N.D. Cal. May 23, 2007).

105. *See, e.g.*, *Smith*, 920 N.E. 2d at 954.

106. *See, e.g.*, *id.*

107. *Compare* United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) *with* United States v. Park, No. CR 05-375SI, 2007 WL 1521573 *1, *8 (N.D. Cal. May 23, 2007).

108. *See infra* Part IV.B.

109. Arizona v. Gant, 556 U.S. 332 (2009).

110. United States v. Jones, 132 S. Ct. 945 (2012).

111. *See* discussion *infra* Part IV.B.

112. *Id.*

ers proceeded to search his car.[113] The officers discovered cocaine in the pocket of a jacket that was located on the back seat.[114] At trial, the defendant moved to suppress the cocaine on the grounds that the warrantless search violated the Fourth Amendment because he was already handcuffed in the back of the patrol car and posed no threat to the officers.[115] Recognizing that the officers had no probable cause for the search, the trial court, nonetheless, denied the motion to suppress and held that the search was permissible as a search incident to arrest.[116] The Supreme Court eventually heard the propriety of the admission of the cocaine into evidence.

The Supreme Court, in an opinion authored by Justice Stevens, began its analysis by reaffirming the base rule that searches incident to arrest are applicable only to areas within the arrestee's immediate control, "meaning 'the area from within which he might gain possession of a weapon or destructible evidence.'"[117] Ultimately, the Court held the search was improper under the search incident to arrest exception, and the evidence should have been suppressed at trial. The Court reasoned, "Police may search a vehicle incident to a recent occupant's arrest only if the arrestee is within reaching distance of the passenger compartment at the time of the search or it is reasonable to believe the vehicle contains evidence of the offense of arrest."[118] Specifically, this holding applies law enforcement's ability to search all containers located within the vehicle for evidence.[119]

In *Jones*, the FBI suspected the defendant of conspiracy in trafficking narcotics in the District of Columbia.[120] As part of its investigation, the FBI received a warrant to use an electronic tracking device on a car belonging to the defendant's wife.[121] Although the warrant authorized the FBI to use and install the GPS device within ten days in the District of Columbia, the FBI agents installed the device on the eleventh day and outside the District of Columbia.[122] Before trial, the defendant moved to suppress the evidence obtained through the GPS device.[123] While the district court suppressed the data that was obtained while the vehicle was

113. *Gant*, 556 U.S. at 335.
114. *Id.*
115. *Id.* at 336–37.
116. *Id*. at 337.
117. *Id.* at 335 (quoting Chimel v. California, 395 U.S. 752, 763 (1969)).
118. *Id.* at 351.
119. *See id.*at 345–51.
120. United States v. Jones, 132 S. Ct. 945, 948 (2012).
121. *Id.*
122. *Id.*
123. *Id.*

parked at the defendant's residence, it admitted into evidence data that was gathered while the car was traveling.[124] The district court reasoned that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[125] However, the trial in which this evidence was admitted resulted in a hung jury.[126] Subsequently, a grand jury returned another conspiracy indictment against the defendant, and, this time, the defendant was found guilty.[127] The appellate court reversed the conviction on the grounds that the evidence obtained by the warrantless use of the GPS device violated the Fourth Amendment.[128]

On appeal to the Supreme Court, Justice Scalia, writing for the majority,[129] said that the Court's earlier Fourth Amendment cases attach the Fourth Amendment right to persons, not places, and applied the "reasonable expectation of privacy" test[130] to evaluate alleged violations.[131] Justice Scalia emphasized that when applying the reasonable expectation of privacy test, the Court, at the very least, "must 'assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[132] Citing various cases and reasoning that *Katz* "did not narrow the Fourth Amendment's scope," Justice Scalia said that the Court has "embodied that preservation of past rights in our very definition of 'reasonable expectation of privacy' which we have said to be an expectation 'that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or *to understandings that are recognized and permitted by society*.'"[133] Ultimately, the Supreme Court held that the attachment of the GPS device constituted a search within the meaning of the Fourth Amendment because "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory

124. *Id.*

125. United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006) (quoting United States v. Knotts, 460 U.S. 276, 281–82 (1983)).

126. *Jones*, 132 S. Ct. at 948.

127. *Id.* at 948–49.

128. *Id.* at 949 (citing United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010)).

129. The opinion was joined by Chief Justice Roberts, Justice Kennedy, Justice Thomas, and Justice Sotomayor.

130. Note, again, this is Justice Harlan's *Katz* test. *See supra* text accompanying note 17.

131. United States v. Jones, 132 S. Ct. 945, 950 (2012) (citing Katz v. United States, 389 U.S. 374, 351 (1967)) (additional citations omitted).

132. *Id.* (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).

133. *Id.* at 951 (quoting Minnesota v. Carter, 525 U.S. 83, 88 (1998)) (emphasis added).

test."[134] Thus, the search was unconstitutional for going beyond the parameters set by the warrant because the officers physically attached the GPS device to the vehicle.[135]

Justice Sotomayor, in her concurring opinion, stated that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[136] Justice Sotomayor believed that the "third-party" approach[137] was "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[138] Noting that people routinely disclose everything from phone numbers dialed, to books read, to medications purchased, Justice Sotomayor did not "assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[139] Justice Sotomayor cautioned that under the Supreme Court's current Fourth Amendment jurisprudence, despite societal expectations to privacy, people will only have those interests protected if the Court "ceases to treat secrecy as a perquisite for privacy."[140]

Justice Alito, in his concurring opinion,[141] criticized the majority for not explaining how the attachment of the GPS device fits within the Fourth Amendment's prohibition against "unreasonable searches and seizures."[142] After noting the problems with the majority's "trespass" approach and advocating for an expectation of privacy test, Justice Alito

---

134. *Id.* at 952 (emphasis added). The majority clarified this comment in the following footnote: "Thus, our theory is *not* that the Fourth Amendment is concerned with *any* technical trespass that led to the gathering of evidence. The Fourth Amendment protects against trespassory searches only with regard to those items (persons, houses, papers, and effects) that it enumerates." *Id.* at 953 n.8 (internal citations and quotation marks omitted). Having a trespassory test in addition to the *Katz* test presents an interesting question, which is outside the scope of this Note: If the data contained in the smartphone is not protected under the Fourth Amendment, does the Fourth Amendment at least protect individuals from police physically handling the smartphone to gain access to the information contained therein?

135. *See id.* at 952–54.

136. *Id.* at 957 (Sotomayor, J., concurring).

137. Presumably referencing the third-party doctrine. *See* discussion *infra* Part VI.

138. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

139. *Id.* (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.")) (citing Katz v. United States, 389 U.S. 347, 351 (1967) ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.")).

140. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

141. His concurrence is joined by Justice Ginsburg, Justice Breyer, and Justice Kagan.

142. *Jones*, 132 S. Ct. at 958 (Alito, J., concurring).

recognized that test comes with its own problems.[143] First, "judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the [expectation of privacy] test looks."[144] Second, the test assumes that citizens have a "well-developed and stable set of privacy expectations."[145] However, Justice Alito asserted that technology can drastically change popular expectations to privacy.[146] While he acknowledged that legislatures have the ability to pass legislation to protect privacy interests,[147] Justice Alito pointed out that statutes regulating the use of GPS technology for law enforcement purposes have not become law, and the best the Court could do in the instant case was to evaluate the "degree of intrusion that a reasonable person would not have anticipated."[148] While Justice Alito asserted that the public views the short-term—but not long-term—monitoring of movement on public streets as reasonable, he also recognized that evolving technology continues to entice the average citizen to trade privacy for convenience.[149]

While the opinions of *Gant* and *Jones* seem to call into question expectations to privacy in the current technological era—specifically how societal devaluation of privacy in technology may be eroding the basis for any Fourth Amendment protections—most subsequent scholarly discussion still focuses on how the Supreme Court would likely rule on the search of a smartphone/cell phone under the search incident to arrest exception. Scholars, and for that matter courts, are missing the opportunity to reevaluate whether individuals have a reasonable expectation of privacy in their smartphones.

B. Judicial and Scholarly Analysis of Privacy Expectations Is (Still) Lacking

Post *Gant* and *Jones*, lower courts, if anything, seemed frustrated by the Supreme Court's continued allowance of smartphone/cell phone searches incident to arrest, and its failure to announce a bright-line rule

143. *Id.* at 960–62.

144. *Id.* at 962 (citing Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring)).

145. *Id.*

146. *Id.*

147. *Id.* at 963 (noting congressional passage of 18 U.S.C. §§ 2510–2522 to protect against unwanted intrusions from wiretapping).

148. *Id.* at 964.

149. *Id.* at 963–64 (noting that GPS monitoring in cell phones provides users services ranging from real-time traffic conditions to more social uses, such as finding or avoiding other GPS users).

that all such searches may only be conducted pursuant to a warrant.[150] For example, in *United States v. Gomez*, the court stated:

> Even though we may disagree with the application of [the] post-*Chimel* line of cases to the ever-advancing technology of cell phones, or more specifically to the application of the . . . [container] rule for searches incident to arrest (as limited by *Gant*), we are constrained to apply the law as the Supreme Court currently pronounces it.[151]

Similarly, the court in *United States v. Hill* recognized that cell phones are capable of storing large amounts of personal information, but it was "unwilling to conclude" that cell phone searches are not subject to the search incident to arrest exception without "guidance from the Supreme Court or the Ninth Circuit . . . ."[152] Interestingly, the *Hill* court seemed persuaded by the *Park* decision but was unwilling to act without binding precedent.[153] *Gomez* and *Hill* highlight that courts are cognizant of the advancements in cell phone technology but are unwilling to affirmatively examine the consequences of those advancements; instead, they continue to proceed into search incident to arrest analysis.

After *Gant* and *Jones*, even scholars seemed not to heed the *Jones* concurrences' calls to reexamine the privacy interests in smartphones. In fact, scholars continue to simply focus on the search incident to arrest exception and its application to smartphones/cell phones. For example, according to Sara Corradi, the Supreme Court's reasoning in *Gant* can be directly applied to a person's privacy interest in his or her smartphone.[154] Corradi believes that the reasoning in *Gant*—that searches incident to arrest should be limited to areas that pose an actual risk of officer safety or evidence destruction—applies to "any situation in which officers attempt to conduct a broad search of a suspect's person and effects, despite his expectation of privacy, simply because the suspect has been arrested."[155] Specifically, because all the lower courts have found that individuals have a legitimate expectation of privacy in their cell phones, *Gant*'s reasoning should apply to smartphones.[156] Therefore, the Court should find that a smartphone search is "a gross invasion of privacy, and thus

---

150. *See, e.g.*, United States v. Gomez, 807 F. Supp. 2d 1134, 1146 (S.D. Fla. 2011); United States v. Hill, No. Cr 10-00261 JSW, 2011 WL 90130, at *7 (N.D. Cal. 2011).

151. *Gomez*, 807 F. Supp. 2d at 1146.

152. *Hill*, 2011 WL 90130, at *7.

153. *Id.*

154. Corradi, *supra* note 23, at 953.

155. *Id.*

156. *Id.* at 953–55.

unconstitutional"[157] unless there is a reasonable expectation that evidence incident to the arrest would be found on phone.[158] Essentially, Corradi argues that smartphones and computers are becoming more and more similar; therefore, courts should apply the recognized privacy interest in computers to smartphones.[159] While she notes many technological similarities,[160] Corradi does not consider the most important dissimilarity—smartphones and apps downloaded onto smartphones share much of the user's "private" information. At most, Corradi relies on Justice Sotomayor's concurring comments in *Jones*—that Justice Sotomayor "would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[161] Corradi, in turn, assumes that "[u]nder this theory, individuals should not have less of an expectation of privacy in their smart phones simply due to the amount of information that is shared with the cell phone company or other third parties."[162] Similar to the courts, Corradi does not give full consideration to how modern smartphones are used.

Even in an article titled "The Whole World Contained: How The Ubiquitous Use Of Mobile Phones Undermines Your Right To Be Free From Unreasonable Searches and Seizures," Mina Ford fails to fully examine whether individuals maintain a reasonable expectation of privacy when using smartphones.[163] Ford argues that law enforcement should never be able to search a smartphone without a search warrant, or, put another way, that there should be no warrantless search exception for smartphones at all (this includes the search incident to arrest exception).[164] Ford declares that "[i]t is almost a laughable notion" to believe that society would not recognize a privacy expectation in cell phones as reasonable.[165] Ford assumes that "mobile phone users have exhibited a subjective expectation of privacy in the contents of their mobile phones,"

157. *Id.* at 954.

158. *Id.* at 961–63.

159. *Id.* at 958–59.

160. According to Corradi, the similarities include: the ability to make voice calls over the Internet; the ability to download programs, including messaging programs; and the ability to access stored information on other devices and on cloud drives. *Id.* (internal citations omitted).

161. *Id.* at 955–56 (quoting United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring)).

162. *Id.* at 956.

163. Mina Ford, Note, *The Whole World Contained: How the Ubiquitous Use of Mobile Phones Undermines Your Right To Be Free From Unreasonable Searches and Seizures*, 39 FLA. ST. U. L. REV. 1077 (2012).

164. *Id.* at 1103.

165. *Id.*

and only offers as evidence for such a claim two online articles that criticize a cellular phone company's collection of text messages.[166] But Ford does not critically examine how smartphone users interact with their phones and the data contained therein on a daily basis.

Similar to the problem in the courts, scholarly works seem, at most, to recognize that there may be a question of whether a privacy interest in smartphones exists,[167] but instead proceed to devote their time to the search incident to arrest exception.[168] If the courts and scholars took the time to actually consider the current smartphone and data-sharing paradigm, they may discover that finding a reasonable expectation of privacy is not such an easy task.

V. THE SUPREME COURT MISSED ITS SECOND CHANCE

Indeed, the Supreme Court had a chance to definitively address the issue of whether a reasonable expectation of privacy exists in smartphones in *Riley v. California*;[169] but, again, the Court assumed such an expectation existed and moved straight into a search incident to arrest analysis.[170] *Riley* is actually a consolidated opinion of two different cases addressing the same issue: "[H]ow the search incident to arrest doctrine applies to modern cell phones . . . ."[171] In the first case, police officers

166. *Id.* at 1103 n.175 (citing Indu Chandrasekhar et al., *Phone Hacking: Timeline of the Scandal*, TELEGRAPH (July 23, 2012), http://www.telegraph.co.uk/news/uknews/phone-hacking/8634176/Phone-hacking-timeline-of-a-scandal.html) (citing Adrian Kingsley-Hughes, *Carrier IQ 'May Have' Collected Text Messages*, ZDNET (Dec. 14, 2011, 7:58 PM), http://www.zdnet.com/blog/hardware/carrier-iq-may-have-collected-text-messages/17122).

167. For an interesting example of an argument that as smartphones/cell phones become capable of storing even more information, the privacy interest in those phones necessarily *increases*, see Daniel Zamani, Note, *There's an Amendment For That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones*, 38 HASTINGS CONST. L.Q. 169, 198 (2010) ("The full potential of smart phones has yet to be seen, but it seems certain that their popularity will only continue to grow. As they reach ubiquity, both in society and in people's lives, the expectation of privacy in them will increase.").

168. *See, e.g.*, Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem*, 22 WM. & MARY BILL RTS. J. 601, 602–03 (2013); Margaret M. Lawton, *Warrantless Searches and Smart Phones: Privacy in the Palm of Your Hand?*, 16 UDC/DCSL L. REV. 89, 102–03 (2012); Park, *supra* note 104, at 462; Samuel J. H. Beutler, Note, *The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches Incident to Arrest*, 15 VAND. J. ENT. & TECH. L. 375, 386–90 (2013); Ashley B. Snyder, Comment, *The Fourth Amendment and Warrantless Cell Phone Searches: When is Your Cell Phone Protected?*, 46 WAKE FOREST L. REV. 155, 161–62 (2011).

169. Riley v. California, 134 S. Ct. 2473 (2014).

170. *Id.* at 2482–85.

171. *Id.* at 2484. Even the Court's framing of its issue statement is a testament to the lack of consideration given to whether a Fourth Amendment "search" took place at all as determined

stopped the defendant for driving with expired tags.[172] Upon contact with the defendant, the police officers discovered that he had a suspended license and arrested him.[173] During the search incident to the arrest, the officers found "items associated with the 'Bloods' street gang."[174] This search also included one of the officers seizing a smartphone[175] from the defendant's pants pocket.[176] "The officer accessed information on the phone and noticed that some words (presumably in text messages or a contacts list) were preceded by the letters 'CK'—a label that, he believed, stood for 'Crip Killers,' a slang term for members of the Bloods gang."[177] Two hours later, a detective "specializing in gangs" also went through the phone, "looking for evidence, because . . . gang members will often video themselves with guns or take pictures of themselves with the guns."[178] The detective found a video where the word "Blood" was used as well as pictures of the defendant standing in front of a car that the officers believed to be involved in an earlier shooting.[179]

The defendant was ultimately charged with multiple crimes related to the earlier shooting, an aggravating factor being that the crimes were gang-related.[180] The defendant unsuccessfully moved pre-trial to suppress the evidence obtained from the smartphone on the grounds that the search violated the Fourth Amendment because the officers did not obtain a warrant, and none of the exceptions to the warrant requirement applied.[181] The trial court admitted the smartphone evidence, and the defendant was convicted on all counts.[182] A California appellate court affirmed both the conviction and the evidence admission, holding that the "Fourth Amendment permits a warrantless search of cell phone data incident to an arrest, so long as the cell phone was immediately associated with the arrestee's person."[183]

---

through the reasonable expectations test. *Id.* The Court couches the issue only in the search incident to arrest exception. *Id.*

172. *Id.* at 2480.

173. *Id.*

174. *Id.*

175. *Id.* The Court defined "smart phone" as "cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity." *Id.*

176. *Id.*

177. *Id.*

178. *Id.* at 2480–81.

179. *Id.* at 2481.

180. *Id.*

181. *Id.*

182. *Id.*

183. *Id.* (internal citation omitted).

In the second case, the defendant was arrested after police officers observed him selling drugs from a car.[184] At the police station, an officer seized a "flip phone"[185] from the defendant and noticed that the phone was receiving calls from a source labeled "my house."[186] The officer opened the phone, looked up the phone number associated with "my house," and traced that number to an apartment building.[187] The officers also saw that the phone's wallpaper was a picture of a woman and a baby.[188] The officers then went to the apartment building, saw a mailbox with the defendant's name on it, and observed someone who resembled the woman from the wallpaper through a window.[189] Based on this information, the officers obtained a search warrant for the apartment, where they subsequently found drugs and a gun.[190]

The defendant was charged with multiple drug and firearm crimes.[191] Although the defendant moved to suppress the evidence obtained from the search of the apartment, arguing that "it was the fruit of an unconstitutional search of his cell phone," the trial court denied the motion.[192] As such, the defendant was convicted of all charges.[193] However, the First Circuit reversed the denial of the motion to suppress and vacated the convictions.[194] The First Circuit held that a search warrant for the flip phone was indeed required because "cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant, because of the amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests."[195]

On the facts of these cases, pundits expected the Supreme Court to not just answer whether police officers generally may search a smartphone/cell phone under the search incident to arrest exception, but also to address the implications of modern technology—specifically whether there is a different standard for "flip phones" versus "smart

184. *Id.*

185. *Id.* The Court defined a "flip phone" as "a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone." *Id.*

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.*

191. *Id.* at 2482.

192. *Id.*

193. *Id.*

194. *Id.* (citing United States v. Wurie, 728 F.3d 1 (1st Cir. 2013)).

195. *Id.* (citing *Wurie*, 728 F.3d at 8–11).

phones."[196] However, like the Court's opinions and scholarly articles that came before it, *Riley* missed the chance to address whether there truly was a "search" under the Fourth Amendment and only focused on the search incident to arrest exception.[197] After the Court quoted the Fourth Amendment, it moved directly into analyzing the issue under the search incident to arrest exception.[198] In doing so, the Court stated:

> As the text makes clear, the ultimate touchstone of the Fourth Amendment is "reasonableness." Our cases have determined that where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant. Such a warrant ensures that the inferences to support a search are drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.[199]

As such, while the Court recognized that "modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy,"[200] the Court spent the vast remainder of the opinion solely focused on the search incident to arrest exception.

While acknowledging that the Government "suggested" that "officers should always be able to search a phone's call log,[201] as they did in" the flip phone case at bar, the Court punted analyzing the issue by pointing out that "[t]here is no dispute here that the officers engaged in a search" of the flip phone.[202] In that one sentence, the Supreme Court avoided analyzing the preliminary Fourth Amendment question of whether there was a "search" by discussing (1) does the individual subjected to the search exhibit an actual expectation of privacy, and (2) is

196. *See, e.g.*, Robert Barnes, *Supreme Court to Decide Case on Police Cellphone Searches*, WASH. POST (Jan. 17, 2014), http://www.washingtonpost.com/politics/supreme-court-to-decide-case-on-police-cellphone-searches/2014/01/17/b0f3c61e-7f8a-11e3-93c1-0e888170b723_story.html.

197. *See Riley*, 134 S. Ct. at 2473.

198. *Id.* at 2482.

199. *Id.* (internal citations and quotation marks omitted).

200. *Id.* at 2484.

201. *Id.* at 2492. To support its "suggestion," the Government cited *Smith v. Maryland*, 442 U.S. 735 (1979). *Id. See also* discussion *infra* Part VII.

202. *Riley*, 134 S. Ct. at 2492–93. Indeed, by arguing that the officers should be able to look at the phone's call log, the Government was, in fact, arguing that no "search" under the Fourth Amendment occurred. *Id.*

that expectation "one that society is prepared to recognize as reasonable."[203]

Ultimately, the Court held that police must always get a search warrant before searching a smartphone/cell phone because once law enforcement seizes the phone, there is neither an officer safety concern nor a reason to believe that evidence within the phone would be destroyed before a search warrant could be obtained.[204] As will be discussed in the following two Parts of this Note, the way individuals use the data in their smartphones and consideration of the third-party doctrine should have justified the *Riley* Court in discussing whether a "search" under the Fourth Amendment occurred at all.[205]

VI. SHARING TOO MUCH INFORMATION

As one scholar so aptly stated,

> Many of us are ambivalent about the value of privacy. On the one hand, for example, a lack of privacy is typically the stuff of dystopias. But on the other hand, some limitations on privacy, whatever the justification, give rise among many persons to only modest concern, if not to utter indifference.[206]

Most smartphone users fall more on the "utter indifference" side of this privacy–concern spectrum. Under the current technological paradigm, smartphone users routinely disclose the phone numbers they call, the websites they visit, and the recipients of emails sent.[207] Moreover, smartphone users also share many other aspects of their lives with others, ranging from their locations[208] to even their moods.[209]

---

203. *See supra* notes 13–16 and accompanying text. Interestingly, towards the end of the *Riley* opinion, the Court did come close to discussing third-party doctrine as it applies to information contained in smartphones/cell phones. However, the Court did not actually refer to the "third-party doctrine." For the definition of the third-party doctrine and discussion on its applicability to smartphones, see discussion *infra* Part VII.

204. *Riley*, 134 S. Ct. at 2485–88, 2495.

205. *See* discussion *infra* Parts VI, VII.

206. R. George Wright, *Some Reasons for Our Ambivalence About the Value of Privacy*, 22 B.U. PUB. INT. L.J. 45, 45–46 (2013).

207. *See* United States v. Jones, 132 S. Ct. 945, 957 (Sotomayor, J., concurring).

208. Shane Dingman, *Here I Am! More Smartphone Users Share Geo-location Data: Survey*, THE GLOBE AND MAIL (Sept. 12, 2013, 12:13 PM), http://www.theglobeandmail.com/technology/digital-culture/here-i-am-more-smartphone-users-share-geo-location-data-survey/article14276866/. This article describes the results of a Pew survey, finding that that 30% of persons over the age of 18 enable the geo-location features of their social media accounts to track their location through their cell phones. Moreover, this article asserts individuals find allowing passive geo-location tracking more desirable than pressing a button in an app to announce their location. *See id.* On the other hand, only about 35% of smartphone users have at one point "explicitly turned off" the geo-location features of their phones. *Id.*

As of February 13, 2014, there were 1,132,053 apps in the Android market.[210] Likewise, as of January 2014, Apple's App Store contained 1,100,827 apps.[211] While Apple and Google do not often report on cumulative or daily downloads, as of early 2013, both companies reported approximately 50 billion total app downloads worldwide.[212] Moreover, the frequency of app downloads seems to be increasing exponentially; in a three-month period in 2013, Apple reported 5 billion app downloads, and in a single month in 2013, Android reported 2.5 billion app downloads.[213] On average, an individual smartphone user has installed twenty-six apps.[214] While the sheer number of downloads is impressive, what is really impressive is what the numbers say about society's apathy towards privacy.

Lately, various governments and companies have shown concern over apps that do not disclose their data collection policies. For example, in January 2013, California's Attorney General released a twenty-three-page report on mobile privacy with the intent to improve privacy protections.[215] In California, apps that collect personal information are required to display their privacy policies or face a $2,500 fine per app download.[216] To bring developers in line with California's law, Amazon, Google, Hewlett-Packard, Microsoft, and Research in Motion "agreed to

---

209. *How Are You Feeling? Microsoft's Mood-Sensing Smartphone Can Tell*, GMA NEWS ONLINE, (July 2, 2013, 5:25 PM), http://www.gmanetwork.com/news/story/315610/scitech/technology/how-are-you-feeling-microsoft-s-mood-sensing-smartphone-can-tell. This online article describes Microsoft's efforts to develop a program that senses a cell phone user's mood based on how he or she uses the phone. *See generally id.* In turn, a user's mood could be automatically shared to social networks, allowing others to better know how and when to communicate with the cell phone user. *See id.*

210. *Number of Android Applications*, APPBRAIN, http://www.appbrain.com/stats/number-of-android-apps (last visited Feb. 23, 2014).

211. *App Store Metrics*, POCKETGAMER.BIZ, http://148apps.biz/app-store-metrics/?mpage=appcount (last visited Feb. 23, 2014).

212. Benedict Evans, *How Many Apps Do Android and iOS Users Download?,* BENEDICT EVANS (May 16, 2013), http://ben-evans.com/benedictevans/2013/5/16/how-many-apps-do-android-and-ios-users-download.

213. *Id.*

214. Tony Bradley, *Study Finds Most Mobile Apps Put Your Security and Privacy at Risk*, PC WORLD (Dec. 5, 2013, 09:54 AM), http://www.pcworld.com/article/2068824/study-finds-most-mobile-apps-put-your-security-and-privacy-at-risk.html.

215. KAMALA D. HARRIS, ATT'Y GEN., CAL. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (2013), *available at* https://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

216. Joe Mullin, *CA to App Devs: Get Privacy Policies or Risk $2500-per-download Fines*, ARS TECHNICA (Dec. 4, 2012, 06:10 AM), http://arstechnica.com/tech-policy/2012/12/ca-to-app-devs-get-privacy-policies-or-risk-2500-per-download-fines/.

a set of privacy principles, which include[d] allowing consumers to review the privacy policy for any app before they download it."[217]

The federal government has also taken notice of the lack of privacy policy disclosures in apps. In a study focusing on apps designed for children, the Federal Trade Commission determined that "[t]he mobile app marketplace is growing at a tremendous speed, and many consumer protections, including privacy and privacy disclosures, have not kept pace with this development."[218] The study, looking at a random sample of "kid" apps,[219] found that only 20% of the apps surveyed disclosed any information about the app's privacy practices.[220] However, "60[%] of the surveyed apps collect geolocation, phone number, contacts, call logs, unique identifiers, and other information stored on the device; and send the information to the app developers or to advertising networks, analytics companies, and other third parties."[221]

Combining the research above, of the twenty-six apps on an average user's smartphone, fifteen collect some sort of personal information; of those fifteen apps, the user has only seen approximately five privacy agreements.[222] However, presumably due to California's privacy law and the agreement between the major tech companies, all individuals, not just Californians, are now exposed to privacy policies. Of course, this is not to say that the privacy policies actually protect individuals' private information contained within their smartphones.

---

217. Mathew J. Schwartz, *California Targets Mobile Apps for Missing Privacy Policies*, INFORMATIONWEEK (Oct. 31, 2012, 10:25 AM), http://www.informationweek.com/mobile/California-targets-mobile-apps-for-missing-privacy-policies/d/d-id/1107139?.

218. FED. TRADE COMM'N, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING 3 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.

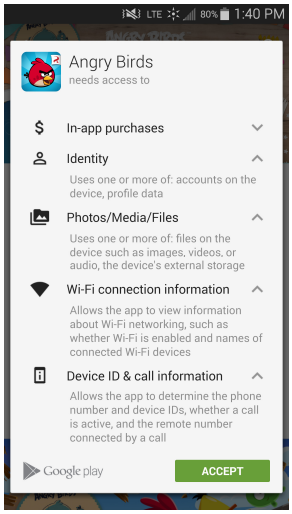
219. *Id.* at A2.

220. *FTC Report Faults Mobile App Makers on Privacy*, FRANKFURT KURNIT KLEIN + SELZ, PC (Jan. 7, 2013), http://fkks.com/news/ftc-report-faults-mobile-app-makers-on-privacy.

221. *Id.*

222. These calculations are for demonstration purposes only. As far as my research has discovered, no one has conducted a study that examines the general population of apps (not just children's apps) and surveyed how often individuals read privacy policies and make the choice of whether or not to download the app based on the privacy policy.

A good example of a privacy policy shown to users before downloading an app is the privacy policy provided for Angry Birds. Within Google Play and on an Android smartphone, one must accept the following information before being allowed to download Angry Birds:



Should a user be determined to look up the privacy policy published on the Rovio Entertainment website,[223] the user would discover that while Rovio says that it maintains the right to disclose collected "non-personal" data from the user's smartphone, Rovio also states it "may employ third party ad serving technologies . . . ."[224] In order to present personalized advertisements to the user, these third parties "may collect and use data . . . including but not limited to, data such as IP address, Device ID, MAC address, installed software, application usage data, hardware type, Operating System information, browser information, unique identifiers in browser cookies, Flash cookies, and HTML5 local storage, Internet and on-line usage information . . . ."[225] Moreover, Rovio does not warrant that these third parties will not use an individual's personal data—that use is subject to the third parties' own terms of service, which the user agrees to by downloading Angry Birds, but is not described in Rovio's Privacy Policy.[226] Indeed, while Rovio provides a link to opt out of some of the "behaviorally targeted advertis-

223. *Who We Are*, ROVIO, http://www.rovio.com/en/about-us/Company (last visited Mar. 17, 2015). Rovio Entertainment is the creator and publisher of Angry Birds.

224. *Privacy Policy*, ROVIO, http://www.rovio.com/privacy (last visited Mar. 17, 2015).

225. *Id.*

226. *See id.*

ing," the user must still "note that the links above may not reach all [of] Rovio's advertising partners and certain behaviorally targeted advertising may still be displayed to you. If you want to be certain that no behaviorally targeted advertisements are displayed to you, please do not use or access the Services."[227] Cynically, these terms may be read as a disclaimer that should an individual download Angry Birds, it is highly likely their personal information will be shared.

Nonetheless, no matter the accuracy of the above calculations, and even if one assumes that smartphone users are exposed to privacy policies for all of their downloaded apps, one principle is clear: people are not deterred by the frequent and wide-ranging collection of their personal data. At a minimum, the formal practice of allowing a developer to gather personal data in exchange for being able to download an app is a widespread practice.

What is to be made, then, of Justices Alito and Sotomayor's comments on privacy interests in the new technological era from *Jones*? If the test is whether the individual being searched exhibits a subjective expectation of privacy and whether society recognizes that expectation as reasonable, the numbers above seriously call into question whether there is an expectation of privacy in smartphones.

VII. TRADITIONAL PHONE PRIVACY JURISPRUDENCE AS THE DOWNFALL OF PRIVACY EXPECTATIONS?

To answer Justices Alito and Sotomayor's calls to reexamine privacy expectations, it seems logical to apply the third-party doctrine from the Court's reasoning in *Smith v. Maryland*.[228] In *Smith*, a telephone company, at law enforcement's request, installed a pen register at its office to track telephone numbers dialed to the victim of a robbery and threatening phone calls.[229] Law enforcement did not get a search warrant before the pen register was installed.[230] The pen register eventually led to an arrest; however, the defendant moved to suppress all information derived from the pen register on the grounds that its use constituted a warrantless search.[231] The Supreme Court held that the use of the pen register did not constitute a search under the Fourth Amendment.[232]

---

227. *Id.*

228. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

229. *Id.* at 737. A pen register is a device that records numbers dialed on a traditional telephone. *Id.* at 736 n.1.

230. *Id.* at 737.

231. *Id.*

232. *Id.* at 745–46.

The Supreme Court reasoned that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through the telephone company switching equipment that their calls are completed."[233] Moreover, the Court stated that "[a]ll subscribers realize . . . that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills."[234] Because of this knowledge, the Supreme Court concluded that it is "too much to believe" that people "harbor any general expectation that the numbers they dial will remain secret."[235]

Even further, the Supreme Court held that a privacy expectation in numbers dialed is not "one that society is prepared to recognize as 'reasonable.'"[236] This conclusion was based on the rule that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[237] The Court explained that individuals risk the information they convey to third parties being disclosed to the government, even if the information was "revealed on the assumption that it [would] be used only for a limited purpose and the confidence placed in the third party [would] not be betrayed."[238] In *Smith*, the defendant voluntarily conveyed his phone number when he placed the phone call.[239] Therefore, there was no "search" under the Fourth Amendment because the defendant expected the phone company was storing his phone number and because he voluntarily disclosed his number to the phone company.[240]

Under the reasoning in *Smith*, it is difficult to see how a reasonable expectation of privacy exists in smartphones. Indeed, this was the exact concern expressed by Justice Sotomayor in *Jones*.[241] As recently as 2006, a federal district court applied *Smith* and held that there was no privacy expectation in phone numbers dialed from cell phones.[242] With a consistent application of the doctrine, this reasoning would extend to all information shared from one's smartphone. With more than half of all apps collecting personal data, a California law requiring app developers to clearly display privacy policies, and the major tech companies agreeing

233. *Id.* at 742.

234. *Id.*

235. *Id.* at 743.

236. *Id.* (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

237. *Id.* at 743–44 (internal citations omitted). Without explicitly naming it, the Court was defining and invoking the third-party doctrine.

238. *Id.* at 744 (citing United States v. Miller, 425 U.S. 435, 443 (1979)).

239. *Id.*

240. *Id.* at 745–46.

241. *See supra* notes 136–38 and accompanying text.

242. Beckwith v. Erie County Water Authority, 413 F. Supp. 2d 214, 224 (2006).

to allow consumers to review privacy polices before download—all with the knowledge that people are not deterred in continuing to download apps and share information—it may be "too much to believe" that people harbor any subjective privacy expectations in information stored in their smartphones.[243] Society may have very well come to the point where people have been enticed to trade privacy for convenience.[244]

Applying the third-party doctrine to all information contained in smartphones is not necessarily that far-fetched. In 2010, the Fifth Circuit held that a party may not have a reasonable expectation of privacy in "subscriber information" due to the third-party doctrine.[245] In *United States v. Bynum*, the defendant had no subjective privacy expectation to his name, email address, telephone number, and physical address because he "voluntarily conveyed all this information to his internet and phone companies . . . [and] 'assumed the risk that th[os]e company[ies] would reveal [that information] to police.'"[246] Sharing subscriber information is no different from allowing an app to access information on one's smartphone in exchange for use of that app. Therefore, under the reasoning of *Bynum*, there may be no reasonable expectation of privacy in smartphones.

Similarly, since the Supreme Court's decision in *Jones*, a federal district court in Maryland applied the third-party doctrine to GPS information obtained from a cell phone.[247] In *United States v. Graham*, the court held that GPS locations provided by cell phones[248] fell squarely under the third-party doctrine and were subject to warrantless searches.[249] *Graham* provides that even without fully reexamining whether a reasonable privacy interest in individuals' smartphones exists, courts are willing to apply the third-party doctrine to smartphone/cell phone searches. While *Bynum* and *Graham* are examples of the furtherance of the third-party doctrine and not necessarily specific analyses of reasonable expectations to privacy, they give notice to people to no longer expect that the Fourth Amendment protects their smartphones' information. Put another way, the more courts widen existing warrantless search exceptions, the

243. *Smith*, 442 U.S. at 743.

244. *See* United States v. Jones, 132 S. Ct. 945, 963–64 (Alito, J., concurring).

245. United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010). "Subscriber information" is information that a user provides to a company—in this case, Yahoo—for the privilege of maintaining a user profile and account. *See id.* at 162, 164.

246. *Id.* at 164 (quoting Smith v. Maryland, 442 U.S. 735, 744 (1979)).

247. United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012).

248. In this case, the GPS location was provided by the cell phone connecting to regional towers, not through modern GPS technology. *Id.* at 387.

249. *Id.* at 400.

more people should not have a reasonable expectation of privacy in their smartphones to begin with.

VIII. CONCLUSION

The courts' jurisprudence and scholars' writings on reasonable expectations to privacy in smartphones are unsatisfactory. These sources either simply assume that there is a reasonable expectation of privacy or do not give the question adequate analysis. While the Supreme Court itself has avoided the issue, concurrences by Justices Sotomayor and Alito open the door for lower courts and scholars to take up the task. However, the topic is still largely under-examined.

In light of advancements in smartphone technology, how people use their smartphones, and what people give up in exchange for such uses, courts need to reexamine whether there is any longer a reasonable expectation of privacy in the smartphone era.[250] An initial application of the reasonable expectation test, à la the third-party doctrine, suggests that there may not be any such expectation. Courts and scholars need to step back, take notice of the important changes in smartphone use and technology, and carefully address the important question of whether there is, in fact, a reasonable expectation of privacy in smartphones.

250. Exactly how the courts should rule on this issue is beyond the scope of this Note. For an interesting discussion on the various methods the courts could use to determine reasonable expectations, see Daniel T. Pesciotta, *I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century*, 63 CASE W. RES. L. REV. 187 (2012).